Available online at www.sciencedirect.com
SCIENCE DIRECT®
JOURNAL OF
A l

www.elsevier.com/locate/jalgebra

Minimal sumsets in infinite abelian groups

Shalom Eliahou [a,*], Michel Kervaire [b]

[a] *Département de Mathématiques, LMPA Joseph Liouville, Université du Littoral Côte d'Opale, Bâtiment Poincaré, 50, rue Ferdinand Buisson, BP 699, 62228 Calais, France*
[b] *Département de Mathématiques, Université de Genève, 2-4, rue du Lièvre, BP 240, 1211 Genève 24, Switzerland*

Received 12 March 2004

Available online 25 March 2005

Communicated by Michel Broué

Abstract

We give a closed formula for the minimal sumset size function

$$\mu_G(r,s)=\min\{|A+B|\colon\ A,B\subset G,\ |A|=r,\ |B|=s\}$$

of an arbitrary (possibly infinite) abelian group G.

1. Introduction

Let G be a group, written additively. Given positive integers $r,s\leqslant|G|$, we denote by

$$\mu_G(r,s)=\min\bigl\{|A+B|\colon\ A,B\subset G,\ |A|=r,\ |B|=s\bigr\}$$

the minimal cardinality of the sumsets

$$A+B=\{a+b\colon\ a\in A,\ b\in B\},$$

where A,B range over all subsets of G with respective cardinalities $|A|=r$ and $|B|=s$.

* Corresponding author.
E-mail addresses: eliahou@lmpa.univ-littoral.fr (S. Eliahou), michel.kervaire@math.unige.ch (M. Kervaire).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.02.014

The function μ_G has been completely determined so far in the case where G is a finite abelian group. The result reads as follows.

Theorem 1 [EKP]. *Let G be a finite abelian group of order n. Then*

$$\mu_G(r,s) = \min_{d|n}\left(\left\lceil \frac{r}{d}\right\rceil + \left\lceil \frac{s}{d}\right\rceil - 1\right)d$$

for all $1 \leqslant r, s \leqslant n$.

Note that, as a particular case, this statement implies the well known Cauchy–Davenport theorem, according to which $\mu_G(r,s) = \min\{r+s-1, p\}$ for G cyclic of prime order p.

Our purpose in this note is to extend the above result to the case of an arbitrary abelian group, including an infinite one. In order to state the result, we need the following key concept from [EK1], which we used there to deal with sumset sizes in non-commutative groups.

Notation. Given a group G, we denote by $\mathcal{H}(G)$ the set of orders of finite subgroups of G, i.e.,

$$\mathcal{H}(G) = \{h \in \mathbb{N}\colon\ h \text{ is the order of a finite subgroup of } G\}.$$

Note that, if G is finite of order n, then $\mathcal{H}(G)$ is a subset of the set $\mathcal{D}(n)$ of positive divisors of n, with equality $\mathcal{H}(G) = \mathcal{D}(n)$ when G is abelian.

On the other hand, if G is torsion-free then $\mathcal{H}(G) = \{1\}$, and conversely.

Our main result in this note is the following.

Theorem 2. *Let G be an arbitrary abelian group. Then,*

$$\mu_G(r,s) = \min_{h\in\mathcal{H}(G)}\left(\left\lceil \frac{r}{h}\right\rceil + \left\lceil \frac{s}{h}\right\rceil - 1\right)h$$

for all positive integers r, s such that $1 \leqslant r, s \leqslant |G|$.

When G is finite abelian, this reduces to Theorem 1. Our methods and proofs in this note are similar to those of [EKP].

2. The small sumsets property

Our proof of Theorem 2 will use the following condition on a group F, ensuring that F contains sufficiently many small sumsets in an appropriate sense.

Definition. Let F be a group. We say that F has the *small sumsets property* if, for every positive integers $r, s \leqslant |F|$, one has

$$\mu_F(r, s) \leqslant r + s - 1.$$

In other words, a group F has the small sumsets property if for every positive integers $r, s \leqslant |F|$, there exist subsets $A, B \subset F$ with $|A| = r$ and $|B| = s$, whose sumset $A + B$ satisfies $|A + B| \leqslant |A| + |B| - 1 = r + s - 1$.

There are several papers dealing with structural properties of sumsets $A + B$ satisfying the condition $|A+B| \leqslant |A|+|B|-1$ (see, e.g., Vosper [V], Kemperman [K2], Hamidoune [H], Lev [L], etc.).

However, the small sumsets property in itself does not seem to have been considered in the literature prior to [EKP].

It is easy to see that cyclic groups have the small sumsets property. Indeed, under the natural ordering of the cyclic group C, the sumset of any two initial segments I, J in C satisfies the condition $|I + J| \leqslant |I| + |J| - 1$. Similarly, any group containing a copy of $\mathbb{Z}$ has the small sumsets property.

We shall now show that all abelian groups have the small sumsets property, a fact which will be used in Section 3. This will follow easily from the next lemma.

Lemma 3. *Let F be a group with the small sumsets property, and let $C = \mathbb{Z}/n\mathbb{Z}$. Then $C \times F$ has the small sumsets property.*

Proof. If F is infinite, then obviously any group containing F also has the small sumsets property. We may thus assume that F if finite, say of order $|F| = d$. Let $r, s \leqslant |C \times F| = n \cdot d$ be positive integers. Consider the euclidean division of r, s by d:

$$r = r_1 d + r_2, \qquad s = s_1 d + s_2$$

with $0 \leqslant r_2, s_2 \leqslant d - 1$. Choose subsets $A, B \subset C \times F$ of the form

$$A = (A_1 \times F) \cup \big(\{a\} \times A_2\big), \qquad B = (B_1 \times F) \cup \big(\{b\} \times B_2\big),$$

where $A_1 \cup \{a\}$, $B_1 \cup \{b\} \subset C$, $A_2, B_2 \subset F$, and with $|A_i| = r_i$ and $|B_i| = s_i$ for $i = 1, 2$. Thus $|A| = r_1 d + r_2 = r$, and similarly $|B| = s_1 d + s_2 = s$.

Ordering $C = \mathbb{Z}/n\mathbb{Z}$ in the natural way, we choose A_1 and $A_1 \cup \{a\}$, more specifically, to be the initial segments in C of length r_1 and $r_1 + 1$, respectively. Similarly, B_1 and $B_1 \cup \{b\}$ are chosen as the initial segments in C of length s_1 and $s_1 + 1$, respectively. Now, given that F possesses the small sumsets property, we may assume that $A_2, B_2 \subset F$, if not both empty, satisfy

$$|A_2 + B_2| \leqslant |A_2| + |B_2| - 1 = r_2 + s_2 - 1.$$

We claim that $|A + B| \leqslant |A| + |B| - 1$.

If A_2, B_2 are both empty, the proof of the claimed inequality is straightforward and left to the reader. Assume now that either A_2 or B_2 is non-empty, so that $|A_2+B_2| \leqslant r_2+s_2-1$ by the above assumption. We have

$$A + B \subset \bigl(\bigl(A_1 \cup \{a\} + B_1\bigr) \times F\bigr) \cup \bigl(\bigl(A_1 + B_1 \cup \{b\}\bigr) \times F\bigr) \cup \bigl(\{a+b\} \times (A_2 + B_2)\bigr),$$

as easily checked. A key point is to note that, in $C = \mathbb{Z}/n\mathbb{Z}$, a sumset of initial segments *is again an initial segment*. Thus, either $A_1 \cup \{a\} + B_1$ contains $A_1 + B_1 \cup \{b\}$, or else it is contained in $A_1 + B_1 \cup \{b\}$. By symmetry, we may assume that $A_1 \cup \{a\} + B_1$ contains $A_1 + B_1 \cup \{b\}$. It follows that

$$A + B \subset \bigl(\bigl(A_1 \cup \{a\} + B_1\bigr) \times F\bigr) \cup \bigl(\{a+b\} \times (A_2 + B_2)\bigr).$$

Hence, $|A+B| \leqslant (r_1+s_1)d + (r_2+s_2-1) = r+s-1$, as desired. $\square$

Proposition 4. *Let G be an abelian group. Then G has the small sumsets property.*

Proof. If G is finite, then it is a product of finite cyclic groups, and hence G has the small sumsets property by a repeated application of Lemma 3. If G is infinite, then either it contains a copy of $\mathbb{Z}$, or else it contains finite subgroups of arbitrarily large cardinality. In either case, it follows from the above that G has the small sumsets property. $\square$

We end this section with a few remarks. A suitable modification of the proof of Lemma 3 yields the following more general statement.

Lemma 5 [EK3]. *Let $0 \to F \to G \to C \to 0$ be a short exact sequence of groups written additively. Assume that F has the small sumsets property, and that C is cyclic. Then, G has the small sumsets property.*

It is conceivable that the above statement remains true under the weaker hypothesis that C, no longer assumed cyclic, still possesses the small sumsets property. However, we currently have no proof for this stronger version, if at all valid.

Here is a straightforward consequence of Lemma 5.

Proposition 6 [EK3]. *Let G be a finite solvable group. Then G has the small sumsets property.*

Neither Lemma 5 nor Proposition 6 will be used in the remainder of this note. But this leaves us with the following question.

Problem. What groups have the small sumsets property?

Perhaps all groups have in fact this property. Some people, however, tend to believe that most finite symmetric groups, for instance, do *not* have the small sumsets property. This is a widely open problem at the date of writing.

3. The main result

We shall restate and then prove Theorem 2, the main result of this note.

Theorem 2. *Let G be an abelian group and $\mathcal{H}(G)$ the set of orders of the finite subgroups of G. Then,*

$$\mu_G(r,s) = \min_{h\in\mathcal{H}(G)}\left(\left\lceil\frac{r}{h}\right\rceil + \left\lceil\frac{s}{h}\right\rceil - 1\right)h$$

for all positive integers $r, s \leqslant |G|$.

In order to discuss the strategy of the proof, we introduce a notation for the right-hand side of the formula, namely

$$\kappa_G(r,s) = \min_{h\in\mathcal{H}(G)}\left(\left\lceil\frac{r}{h}\right\rceil + \left\lceil\frac{s}{h}\right\rceil - 1\right)h.$$

There are two separate parts in the proof. In the first one, we use Kneser's theorem to show that $\mu_G(r,s)$ is bounded below by the function $\kappa_G(r,s)$. In the second one, we explicitly construct subsets of G, of given cardinalities r, s, whose sumset is of size given by $\kappa_G(r,s)$, thus establishing the reverse inequality $\mu_G(r,s) \leqslant \kappa_G(r,s)$.

Proof. We first prove that $\mu_G(r,s) \geqslant \kappa_G(r,s)$. Let $A, B \subset G$ be any subsets with $|A| = r$ and $|B| = s$. By Kneser's theorem, there exists a finite subgroup $H \leqslant G$ such that

$$|A+B| \geqslant |A+H| + |B+H| - |H|.$$

(An explicit subgroup H satisfying this inequality is the stabilizer of the sumset $A+B$, that is $H = \mathrm{Stab}(A+B) = \{g \in G\colon\ A+B+g = A+B\}$.) Factoring $|H|$ in the above inequality, we may rewrite it as

$$|A+B| \geqslant \left(\frac{|A+H|}{|H|} + \frac{|B+H|}{|H|} - 1\right)|H|.$$

The key point now is to observe that $A+H$ is a disjoint union of H-cosets. It follows that the fraction $|A+H|/|H|$ is an integer, obviously greater than or equal to $|A|/|H|$. Hence, $|A+H|/|H| \geqslant \lceil |A|/|H| \rceil = \lceil r/m \rceil$, where $m = |H|$. Similarly, $|B+H|/|H| \geqslant \lceil s/m \rceil$. It follows that

$$|A+B| \geqslant \left(\left\lceil\frac{r}{m}\right\rceil + \left\lceil\frac{s}{m}\right\rceil - 1\right)m.$$

Given that m, the order of H, belongs to the set $\mathcal{H}(G)$, we have

$$|A+B| \geqslant \min_{h\in\mathcal{H}(G)}\left(\left\lceil\frac{r}{h}\right\rceil + \left\lceil\frac{s}{h}\right\rceil - 1\right)h.$$

The stated inequality,

$$\mu_G(r,s) \geqslant \min_{h\in\mathcal{H}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h,$$

follows.

It remains to show that $\mu_G(r,s) \leqslant \kappa_G(r,s)$. Let $m \in \mathcal{H}(G)$, and let $H \leqslant G$ be a subgroup of G of order m. Let $\pi : G \to G/H$ denote the canonical quotient map. Let also $r_0 = \lceil r/m \rceil$ and $s_0 = \lceil s/m \rceil$. Since the group G/H, being abelian, has the small sumsets property, we have $\mu_{G/H}(r_0, s_0) \leqslant r_0 + s_0 - 1$. Thus, there exist subsets $A_0, B_0 \subset G/H$, of cardinality r_0, s_0, respectively, such that

$$|A_0 + B_0| \leqslant r_0 + s_0 - 1.$$

Let $A = \pi^{-1}(A_0)$, $B = \pi^{-1}(B_0)$. Then, A, B are subsets of G of cardinality $r_0 m$, $s_0 m$, respectively. Since $A + B = \pi^{-1}(A_0 + B_0)$, we also have $|A + B| = |A_0 + B_0| m$.

Thus, $|A + B| = |A_0 + B_0| m \leqslant (r_0 + s_0 - 1)m$, and hence

$$\mu_G(r_0 m, s_0 m) \leqslant (r_0 + s_0 - 1)m.$$

Given that $r \leqslant r_0 m$, $s \leqslant s_0 m$, it is clear that $\mu_G(r,s) \leqslant \mu_G(r_0 m, s_0 m)$. Summarizing, we have

$$\mu_G(r,s) \leqslant \mu_G(r_0 m, s_0 m) \leqslant (r_0 + s_0 - 1)m = \left(\left\lceil \frac{r}{m} \right\rceil + \left\lceil \frac{s}{m} \right\rceil - 1 \right) m.$$

As $m \in \mathcal{H}(G)$ was chosen arbitrary, the stated inequality,

$$\mu_G(r,s) \leqslant \min_{h\in\mathcal{H}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h,$$

follows. □

4. A strengthening of Theorem 2

We shall now show, using Theorem 2, that $\mu_G(r,s)$ may always be realized in an abelian group G by sets $A, B \subset G$ such that $A \subset B$. As will be shown in the last section, this is no longer true in general in the non-abelian context.

Proposition 7. *Let G be an abelian group. Then, for every positive integers r, s such that $1 \leqslant r \leqslant s \leqslant |G|$, there exist subsets $A, B \subset G$ with $|A| = r$, $|B| = s$ and $A \subset B$, such that $|A + B| = \mu_G(r,s)$.*

Proof. We shall use a result from [EKP] and refine the proof of Theorem 2. Let $m \in \mathcal{H}(G)$ be such that $\mu_G(r,s) = (\lceil r/m \rceil + \lceil s/m \rceil - 1)m$, and let $H \leqslant G$ be a subgroup of G of order m. As in the second part of the proof of Theorem 2, let $r_0 = \lceil r/m \rceil$, $s_0 = \lceil s/m \rceil$ and $\pi : G \to G/H$ the canonical quotient map. Clearly, we have $r_0 \leqslant s_0$. We know that $\mu_{G/H}(r_0, s_0) \leqslant r_0 + s_0 - 1$, as all abelian groups have the small sumsets property. Hence, G/H contains subsets A_0, B_0 of cardinality r_0, s_0, respectively, such that $|A_0 + B_0| \leqslant r_0 + s_0 - 1$. We claim that we may choose A_0, B_0 in such a way that A_0 will be contained in B_0. In order to do so, we proceed as follows.

First, if G/H contains a copy of $\mathbb{Z}$, then the initial segments $A_0 = \{0, \ldots, r_0 - 1\}$, $B_0 = \{0, \ldots, s_0 - 1\}$ in $\mathbb{N} \subset G/H$ have the required properties.

Otherwise, if G/H does not contain any copy of $\mathbb{Z}$, then since $|G/H| \geqslant s_0$, there must be a finite subgroup $K_0 \leqslant G/H$ of cardinality $|K_0| \geqslant s_0$. We decompose K_0 as a product of cyclic groups $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, order K_0 lexicographically with respect to this decomposition, and take for A_0, B_0 the initial segments in K_0 of cardinality r_0, s_0, respectively. Thus, $A_0 \subset B_0$, and $|A_0 + B_0| \leqslant r_0 + s_0 - 1$ as stated by the proposition in [EKP, Section 2, p. 340].

The inverse images $\pi^{-1}(A_0), \pi^{-1}(B_0)$ have cardinality $r_0 m, s_0 m$, respectively. Note that $r \leqslant r_0 m$ and $s \leqslant s_0 m$, by definition of r_0, s_0. Hence, we may choose a subset A of cardinality r such that $A \subset \pi^{-1}(A_0)$ and also, since $r \leqslant s$, a subset B of cardinality s such that $A \subset B \subset \pi^{-1}(B_0)$. It follows that $|A + B| \leqslant |\pi^{-1}(A_0) + \pi^{-1}(B_0)| = |\pi^{-1}(A_0 + B_0)| = |A_0 + B_0| m \leqslant (r_0 + s_0 - 1)m = (\lceil r/m \rceil + \lceil s/m \rceil - 1)m = \mu_G(r, s)$. Thus $|A + B| = \mu_G(r, s)$ by minimality of $\mu_G(r, s)$, and $A \subset B$ by construction. □

5. A remark on the non-abelian case

It is natural to ask to what extent the formula

$$\mu_G(r, s) = \min_{h \in \mathcal{H}(G)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h$$

remains valid for a non-abelian group G. We have shown that this formula still holds for the alternating group $\mathcal{A}_4$ [EK1], and for the dihedral group D_{p^n} of cardinality $2p^n$, where p is a prime number [EK2]. We also know that this formula for μ_G *does not hold* for the non-abelian group G of order 21 with the presentation $G = \langle a, b\colon\ a^7 = b^3 = 1, bab^{-1} = a^2 \rangle$. (In this example, the formula fails for exactly four pairs $\{r, s\}$, namely $\{6, 8\}, \{6, 9\}, \{8, 9\}$ and $\{9, 9\}$.) Finally, this formula also holds for a torsion-free group G, in which case it reduces to $\mu_G(r, s) = r + s - 1$ since $\mathcal{H}(G) = \{1\}$. The fact that $\mu_G(r, s) = r + s - 1$ in a non-abelian torsion-free group G follows from the corollary to [K1, Theorem 5], according to which $|A + B| \geqslant |A| + |B| - 1$ for any finite non-empty subsets A, B of G. This yields the inequality $\mu_G(r, s) \geqslant r + s - 1$. The reverse inequality $\mu_G(r, s) \leqslant r + s - 1$ is valid in any group G containing a copy of $\mathbb{Z}$.

However, a difference between the abelian and the non-abelian case arises if one considers minimal sumsets of the form $A + A$. To illustrate this, we introduce the function

$$\mu_G(r) = \min\bigl\{ |A + A|\colon\ A \subset G,\ |A| = r \bigr\}.$$

It is obvious that $\mu_G(r,r) \leqslant \mu_G(r)$ for all $1 \leqslant r \leqslant |G|$. We claim that the equality $\mu_G(r,r) = \mu_G(r)$ holds if G is abelian. This is an immediate consequence of Proposition 7, as $\mu_G(r,r)$ may then be realized by subsets $A \subset B$ of the same cardinality r, that is by sets $A = B$.

In the non-abelian case, however, there are instances where the strict inequality $\mu_G(r,r) < \mu_G(r)$ occurs, even if the formula for $\mu_G(r,s)$ is given, as in the abelian case, by $\min_{h \in \mathcal{H}(G)}(\lceil r/h \rceil + \lceil s/h \rceil - 1)h$. One specific example is the alternating group $G = \mathcal{A}_4$. As already stated, we know that

$$\mu_{\mathcal{A}_4}(r,s) = \min_{h \in \mathcal{H}(\mathcal{A}_4)} \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h,$$

where $\mathcal{H}(\mathcal{A}_4) = \{1,2,3,4,12\}$. Taking $r = 6$, we have $\mu_{\mathcal{A}_4}(6,6) = 9$ as follows from [EK1, Theorem 4.2].

One way to realize $\mu_{\mathcal{A}_4}(6,6)$ is as follows. Let $H \leqslant \mathcal{A}_4$ be a subgroup of order 3, and let $x_1, x_2, x_3, x_4 \in \mathcal{A}_4$ be such that the four right cosets Hx_1, Hx_2, Hx_3, Hx_4 constitute a partition of $\mathcal{A}_4$. Let $A = Hx_1 \cup Hx_2$ and $B = x_3^{-1}H \cup x_4^{-1}H$. Then $|A| = |B| = 6$, and $A \cdot B = \mathcal{A}_4 \setminus H$, the complement of H in $\mathcal{A}_4$, so that $|A \cdot B| = 9$.

However, $\mu_{\mathcal{A}_4}(6) = 10$. Indeed, a simple computer experiment reveals that, among the 924 subsets $X \subset \mathcal{A}_4$ of size $|X| = 6$, there are 12 instances where $|X \cdot X| = 10$, 24 instances where $|X \cdot X| = 11$, and the 888 remaining subsets X satisfy $X \cdot X = \mathcal{A}_4$. The structure of the 12 subsets of size 6 with productset of minimal size 10 is as follows. Let $V \leqslant \mathcal{A}_4$ be the unique subgroup of order 4, which is normal, let $P \subset V$ be any subset of cardinality 2, and let C be one of the two cosets of V distinct from V. Let $X = P \cup C$. In cycle notation,

$$X = P \cup \left\{(1,2,3)^{\epsilon}, (1,2,4)^{-\epsilon}, (1,3,4)^{\epsilon}, (2,3,4)^{-\epsilon}\right\}$$

with $\epsilon = 1$ or -1. Then, $|X| = 6$ and $|X \cdot X| = 10$. The 12 subsets X of $\mathcal{A}_4$ with these two properties are all of the above form $P \cup C$, with 6 choices for the pair $P \subset V$ and 2 independent choices for the coset C. The fact that $|X \cdot X| = 10$ follows from the following relations: $C \cdot C = C^{-1}$, $P \cdot C = C \cdot P = C$, and $P \cdot P = P$ or $V \setminus P$.

Acknowledgment

During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

References

[EK1] S. Eliahou, M. Kervaire, Some results on minimal sumset sizes in finite non-abelian groups, preprint, 2002.

[EK2] S. Eliahou, M. Kervaire, Sumsets in dihedral groups, European J. Combin., in press.

[EK3] S. Eliahou, M. Kervaire, The small sumsets property for solvable finite groups, European J. Combin., in press.

[EKP] S. Eliahou, M. Kervaire, A. Plagne, Optimally small sumsets in finite abelian groups, J. Number Theory 101 (2003) 338–348.

[H] Y.O. Hamidoune, On small subset product in a group, in: Structure Theory of Set Addition, Astérisque 258 (1999) 281–308.

[K1] J.H.B. Kemperman, On complexes in a semigroup, Indag. Math. 18 (1956) 247–254.

[K2] J.H.B. Kemperman, On small sumsets in an abelian group, Acta Math. 103 (1960) 63–88.

[L] V.F. Lev, On small sumsets in an abelian group, in: Structure Theory of Set Addition, Astérisque 258 (1999) 317–321.

[V] A.G. Vosper, The critical pairs of subsets of a group of prime order, J. London Math. Soc. 31 (1956) 200–205; Addendum to "The critical pairs of subsets of a group of prime order", J. London Math. Soc. 31 (1956) 280–282.